Remarks

I. Status of claims

Claims 1-27 were pending. Claims 28-30 have been added.

II. Claim rejections

The Examiner has rejected claims 1-27 under 35 U.S.C. § 102(b) over Schneck (U.S. 5,933,498).

For the purpose of the following discussion, the Examiner is reminded that "for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly" (MPEP § 706.02(a)).

A. Claims 1-11 and 21-27

Claim 1 is an independent claim and claims 2-11 and 21-27 depend from claim 1.

1. Independent claim 1

Claim 1 has been amended and now recites that the controller is configured to authorize wireless transmission of a transfer file to a third party device in accordance with meta-data associated with the particular digital content and without regard to any identifier of the third party device, wherein the transfer file includes meta data containing permissions information restricting rendering of the particular digital content by the third party device. With respect to secondary distribution, Schneck teaches that (col. 25, lines 53-63):

> Transmission of (an unencrypted copy of) the primary distribution data (either to a network or to an output device such as a tape or disk) can only be effected when the system, acting under the rules embodied in the owner's permission list, allows external output. Denial of permission to transmit an unencrypted copy may result in no output or may result in transmission of an encrypted copy (for which the recipient must then negotiate permissions in order to use). Alternatively, denial of permission to transmit may result in the transmission

of random data, thereby denying the user knowledge of whether or not encrypted data was transferred.

Therefore, in response to an attempt to transmit primary distribution data, a user's system first determines what type of data is to be transmitted based on a determination of whether external output is allowed. To this end, the user's system must act "under the rules embodied in the owner's permission list." Table I (col. 11, lines 6-35) shows that the rules, in accordance with which the user's system must act, include a "System Ids/Public keys" field that specifies "other systems to which these rules may be redistributed." Accordingly, in response to an attempt to transmit primary distribution data to a third party system, the user's system must determine whether an identifier of the third party system is specified in the "System Ids/Public keys" field. If the third party system identifier is specified in the "System Ids/Public keys" field, the user's system can transmit an unencrypted copy of the primary distribution data to the third party system. If the third party system identifier is not specified in the "System Ids/Public keys" field, the user's system may transmit no output, an encrypted copy of the primary distribution data, or random data.

Thus, Schneck fails to teach or suggest a portable media device with a controller that is configured to authorize wireless transmission of a transfer file to a third part device without regard to any identifier of the third party device, as recited in claim 1. Indeed, in accordance with Schneck's teaching, the user's system must compare an identifier of the third party device with the identifiers specified in the "System Ids/Public keys" field of the rules in order to determine what type of data to transmit in response to a request to transmit primary distribution data from a user's system.

For at least these reasons, the Examiner's rejection of independent claim 1 under 35 U.S.C. § 102(b) over Schneck should be withdrawn.

2. Claims 2-11 and 21-27

Each of claims 2-11 and 21-27 incorporates the features of independent claim 1 and therefore is patentable for at least the same reasons explained above. Claims 4, 6-10, and 21-28, and 30 also are patentable for the following additional reasons.

a. Claim 4

Claim 4 recites that the controller is configured to confirm a user license based upon a comparison of a user identifier embedded in the meta-data associated with a given digital content with a user identifier stored in the memory. Schneck's system does not confirm a user license based upon such a comparison. To the contrary, in Schneck's approach, a user is granted access to a protected dataset based on whether or not rules permitting access to the dataset are "present, available, and valid" (col. 18, line 23). If such rules are found by the access mechanism 114, access to the dataset is provided – no comparison of user identifiers is performed by Schneck's system to confirm a user license.

The Examiner has cited col. 6, lines 61-67, of Schneck's disclosure to support her rejection of claim 4. The totality of the cited disclosure is as follows:

> Without the tamper detection/reset mechanism of this invention, software can be modified or data can be intercepted rendering useless any attempts at control.
>
> Degrees of protection utilized in the computer system hardware (for example, tamperproof and tamper-detect features) and the cryptographic tools will depend on the nature of the data to be protected as well as the user environment.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to confirm a user license based upon a comparison of a user identifier embedded in the meta-data associated with a given digital content with a user identifier stored in the memory of a portable media device.

b. Claim 6

Claim 6 incorporates the features of claim 4 and therefore is patentable for at least the same reasons. Claim 6 also recites that the controller is configured to enable playback of only a sample of the digital content in response to a failed user license confirmation. Schneck does not expressly or impliedly teach such a feature. Indeed, in accordance with Schneck's access control scheme, playback of protected data is entirely disabled in response to a failed user license confirmation (see, e.g., col. 18, lines 32-43).

The Examiner has cited col. 14, lines 41-50, of Schneck's disclosure to support her rejection of claim 6. The totality of the cited disclosure is as follows:

> Function *f* may, for example, be an inquiry to a certification database or certification authority to obtain the public key so as to ensure that the serial number is authentic. Having determined

> the rule-encrypting key (step S740), encrypt the data key K_D with the calculated rule-encrypting key K_R (step S742) and store the keys (step S744). Next, encrypt the rules using the rule-encrypting key K_R (step S746). The encrypted rules and the encrypted data key K_D are stored as packaged rules 152 for subsequent distribution. The rule-encrypting key K_R may be stored or recalculated from the serial number whenever needed.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to enable playback of only a sample of the digital content in response to a failed user license confirmation.

c. Claim 7

Claim 7 recites that the controller is configured to direct received digital content selectively to unrestricted memory storage or to restricted memory storage based upon a user license confirmation. Schneck does not expressly or impliedly teach such a feature. Indeed, in Schneck's approach, all digital content is stored in restricted (or protected) memory storage regardless of whether a user license is confirmed or not.

The Examiner has cited col. 7, lines 12-19, of Schneck's disclosure to support her rejection of claim 7. The totality of the cited disclosure is as follows:

> The device includes storage means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.
>
> In another aspect, this invention is a method of distributing digital data for subsequent controlled use of the data by a user.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to direct received digital content selectively to unrestricted memory storage or to restricted memory storage based upon a user license confirmation.

d. Claim 8

Claim 8 incorporates the features of claim 7 and therefore is patentable for at least the same reasons. Claim 8 also recites that the controller is configured to direct licensed digital content to unrestricted memory storage and to direct unlicensed digital content to restricted memory storage. Schneck does not expressly or impliedly teach such a feature. Indeed, in accordance with Schneck's access control scheme, both licensed content and unlicensed digital content are handled in the same way.

The Examiner has cited col. 7, lines 23-31, of Schneck's disclosure to support her rejection of claim 8. The totality of the cited disclosure is as follows:

> The method includes protecting portions of the digital data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing the protected portions of the digital data and the protected rules. The user is provided controlled access to the data only in accordance with the rules as enforced by a tamper detecting access mechanism.
>
> In another aspect, this invention is a storage device, readable by a machine, tangibly embodying a package of digital data comprising protected portions of digital data; and rules concerning access rights to the digital data, whereby a user is provided controlled access to the digital data only in accordance with the rules as enforced by a tamper detecting access mechanism.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to direct licensed digital content to unrestricted memory storage and to direct unlicensed digital content to restricted memory storage.

e. Claim 9

Claim 9 incorporates the features of claim 7 and therefore is patentable for at least the same reasons. Claim 9 also recites that the controller is configured to restrict storage of unlicensed digital works to a predetermined quantity. Schneck does not even hint that a controller of a portable media device could be configured to restrict storage of unlicensed digital works to a predetermined quantity. Indeed, Schneck does not teach or suggest anything about restricting the quantity of digital works (whether licensed or unlicensed) that can be stored in a system.

The Examiner has cited col. 7, lines 35-47, of Schneck's disclosure to support her rejection of claim 9. The totality of the cited disclosure is as follows:

> The data represent computer software, text, graphics, audio, and video, alone or in combinations.
>
> The protecting is done by encrypting the portions of the data, and access is prevented to the encrypted portions of the data other than in encrypted form.

> In some embodiments the rules are provided with the data, whereas in others the rules are provided separately. The rules can specify various access rights and controls, including rights of further distribution of the data.
>
> In preferred embodiments, data are destroyed when tampering is detected.
>
> The device containing the mechanism of the present invention can be a stand-alone device such as a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, a computer system or the like.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to restrict storage of unlicensed digital works to a predetermined quantity.

f. Claim 10

Claim 10 incorporates the features of claim 7 and therefore is patentable for at least the same reasons explained above.

g. Claim 21

Claim 21 recites that the controller is configured to control wireless transmission and rendering of a particular digital content based upon a comparison of a user identifier embedded in meta-data associated with the particular digital content with a user identifier stored in the memory. As explained above, Schneck's system does not confirm a user license based upon such a comparison. To the contrary, in Schneck's approach, a user is granted access to a protected dataset based on whether or not rules permitting access to the dataset are "present, available, and valid" (col. 18, line 23). If such rules are found by the access mechanism 114, access to the dataset is provided – no comparison of user identifiers is performed by Schneck's system to confirm a user license.

The Examiner has cited col. 8, lines 11-19, of Schneck's disclosure to support her rejection of claim 21. The totality of the cited disclosure is as follows:

> Examples of the acceptability of such packaging include lap-top computers and the original Macintosh computer, as well as integrated televisions, VCRs and video or audio laser disk players.
>
> Threat: Digital Copying
>
> Countermeasure: Secure Coprocessor

> Selection of a secure coprocessor is indicated to implement protection against unauthorized use when an operating system (OS) is determined to be untrustworthy--that is, when the OS cannot provide adequate resistance to the anticipated threat.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to control wireless transmission and rendering of a particular digital content based upon a comparison of a user identifier embedded in meta-data associated with the particular digital content with a user identifier stored in the memory of a portable media device.

h. Claims 22-24

Claims 22-24 incorporate that features of claim 21 and therefore are patentable for at least the same reasons.

i. Claim 25

Claim 25 recites that the controller is configured to assemble a transfer file comprising an encryption key for decrypting encrypted digital content, to encrypt the transfer file with an encryption key received from a second portable media device, and to cause the encrypted transfer file to be transmitted wirelessly to the second portable media device. Schneck does not expressly or impliedly teach such a feature. Schneck does not teach or suggest anything about a controller of a portable media device that is configured to encrypt a transfer file with an encryption key received from a second portable media device. Indeed, in Schneck's approach (col. 12, lines 4-7):

> data-encrypting key, K_D, is the same for all copies of the data. K_D is selected by the distributor and may be different for each product (i.e., for each packaged data 108).

The Examiner has cited col. 8, lines 15-28, of Schneck's disclosure to support her rejection of claim 25. The totality of the cited disclosure is as follows:

> Countermeasure: Secure Coprocessor
>
> Selection of a secure coprocessor is indicated to implement protection against unauthorized use when an operating system (OS) is determined to be untrustworthy--that is, when the OS cannot provide adequate resistance to the anticipated threat. When the OS is untrustworthy, any measures implemented in the OS, or protected by it, can be circumvented through the OS or by-passing it.

> Countermeasure: Detection of Unsealing
>
> The protection provided by a coprocessor could be circumvented by tampering. The coprocessor is protected by tamper detection that causes the rules, cryptographic data, and decrypted protected data to be destroyed.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to assemble a transfer file comprising an encryption key for decrypting encrypted digital content, to encrypt the transfer file with an encryption key received from a second portable media device, and to cause the encrypted transfer file to be transmitted wirelessly to the second portable media device.

j. Claim 26

Claim 26 recites that the controller is configured to change a license status identifier associated with a particular digital content from unlicensed to licensed in response to a determination that a content identifier associated with the particular digital content matches a content identifier stored in the memory and corresponding to a previously licensed digital content file. Schneck expressly teaches that, in his approach, the "system denies the user direct access to manipulate the permissions list" (col. 23, lines 64-65).

The Examiner has cited col. 8, lines 35-42, of Schneck's disclosure to support her rejection of claim 26. The totality of the cited disclosure is as follows:

> Threat: Deliberate Attack via Legacy and Customized Hardware
>
> Countermeasure: Keep the Information on the Coprocessor Board
>
> Access may be controlled if the information leaves the coprocessor board only for output purposes.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to change a license status identifier associated with a particular digital content from unlicensed to licensed in response to a determination that a content identifier associated with the particular digital content matches a content identifier stored in the memory and corresponding to a previously licensed digital content file.

k. Claim 27

Claim 27 recites that the controller is configured to transmit a user identifier assigned to the portable media device to a license manager after each transmission of digital content

information from the portable media device to one or more other devices. Schneck does not even hint that a user identifier is transmitted to a license manager after each transmission of digital content information from the portable media device to one or more other devices. Indeed, in Schneck's approach (col. 12, lines 4-7):

> data-encrypting key, K_D, is the same for all copies of the data. K_D is selected by the distributor and may be different for each product (i.e., for each packaged data 108).

The Examiner has cited col. 8, lines 25-37, of Schneck's disclosure to support her rejection of claim 27. The totality of the cited disclosure is as follows:

> The protection provided by a coprocessor could be circumvented by tampering. The coprocessor is protected by tamper detection that causes the rules, cryptographic data, and decrypted protected data to be destroyed. Both passive and active means are used to effect such destruction. Semiconductor memory is volatile and does not retain data when power is removed. A long-life battery provides energy sufficient to allow rewriting (zeroizing) nonvolatile memory containing, for example, the private key. Without the private key the system will be unable to decrypt any protected data and it must be returned to an authorized service facility for installation of a new private key.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a controller that is configured to transmit a user identifier assigned to the portable media device to a license manager after each transmission of digital content information from the portable media device to one or more other devices.

1. Claims 28 and 30

Regarding claims 28 and 30, Schneck does not expressly or impliedly teach anything about encrypting a transfer file with an encryption key received from a third party device and authorizing wireless transmission of the transfer file from a portable media device to the third party device, as required by these claims.

The Examiner has cited col. 7, lines 12-29 and 34-50, of Schneck's disclosure to support her rejection of claims 28 and 30. The totality of the cited disclosure is as follows:

> The device includes storage means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.

> In another aspect, this invention is a method of distributing digital data for subsequent controlled use of the data by a user. The method includes protecting portions of the digital data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing the protected portions of the digital data and the protected rules. The user is provided controlled access to the data only in accordance with the rules as enforced by a tamper detecting access mechanism.
>
> In another aspect, this invention is a storage device, readable by a machine, tangibly embodying a package of digital data comprising protected portions of digital data; and rules concerning access rights to the digital data, whereby a user is provided controlled access to the digital data only in accordance with the rules as enforced by a tamper detecting access mechanism.
>
> The data represent computer software, text, graphics, audio, and video, alone or in combinations.
>
> The protecting is done by encrypting the portions of the data, and access is prevented to the encrypted portions of the data other than in encrypted form.
>
> In some embodiments the rules are provided with the data, whereas in others the rules are provided separately. The rules can specify various access rights and controls, including rights of further distribution of the data.
>
> In preferred embodiments, data are destroyed when tampering is detected.
>
> The device containing the mechanism of the present invention can be a stand-alone device such as a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, a computer system or the like.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion anything about encrypting a transfer file with an encryption key received from a third party device and authorizing wireless transmission of the transfer file from a portable media device to the third party device, as recited in claims 28 and 30.

m. Conclusion

For at least these additional reasons, the Examiner's rejection of dependent claims 4, 6-10, and 21-28, and 30 under 35 U.S.C. § 102(b) over Schneck should be withdrawn.

B. Claims 12-20

Claim 12 is an independent claim and claims 13-20 depend from claim 12.

1. Independent claim 12

The Examiner has indicated that:

> With respect to claims 12-20, Applicant argues that Schneck does not disclose the allocation of an incentive to a first user or a portable media device licensed to transmit a particular digital content in response to receipt of an indication of a purchase of a license. Applicant's attention is directed to Schneck et al. (US 5,933,498) col 6 ln 48 – col 8 ln 58.

Contrary to the Examiner's assertion that Applicants' arguments have been considered, the Examiner has failed to address Applicants' points regarding the failings of Schneck's teachings with respect to claim 12. Instead, the Examiner merely has copied verbatim her assertions from the prior rejection of claim 12. If the Examiner relies on the teachings of Schneck in her next action, Applicants request that the Examiner give due consideration of and respond directly to all of Applicants' arguments regarding the failings of Schneck's teachings.

In any event, claim 12 has been amended and now recites that the license manager is configured to allocate an incentive having an exchangeable pecuniary value to a first user of a portable media device licensed to transmit a particular digital content in response to receipt of an indication of a purchase of a license for the particular digital content by a second user of a portable media device who received a copy of the particular digital content from the first user. Schneck does not teach or suggest such a feature. There is no disclosure whatsoever in the "Summary of the Invention" section of Schneck's disclosure (which is cited by the Examiner to support her rejection of claim 12) that teaches or suggests anything about a license manager that allocates an incentive having an exchangeable pecuniary value to a first user of a portable media device licensed to transmit a particular digital content in response to receipt of an indication of a purchase of a license for the particular digital content by a second user of a portable media device who received a copy of the particular digital content from the first user.

In order to establish a proper *prima facie* rejection of a claim under 35 U.S.C. § 102, the Examiner must show that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" (MPEP § 2131). The Examiner, however, has failed in this regard as shown by the following detailed analysis of the section of Schneck's disclosure cited by the Examiner in support of her rejection of claim 12 under 35 U.S.C. § 102(b):

Location in Schneck's Disclosure (col./line numbers)	Quoted Text of Schneck's Disclosure	Analysis
6, 48-56	This invention controls access to and use and distribution of data. For example, when the data are in the form of textual and graphical information, this invention can control how much of the information is displayed and in what form; or, when the data represents a computer software program, this invention can control how much of the software's functionality is available. Classified data are similarly controlled.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
6, 57-62	In addition, this invention controls secondary distribution and creation of derivative works. Prior art systems rely on software for security. Without the tamper detection/reset mechanism of this invention, software can be modified or data can be intercepted rendering useless any attempts at control.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
6, 63-67	Degrees of protection utilized in the computer system hardware (for example, tamperproof and tamper-detect features) and the cryptographic tools will depend on the nature of the data to be protected as well as the user environment.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 1-7	In one preferred embodiment, this invention is a method of controlling access to data by protecting portions of the data; determining rules concerning access rights to the data; preventing access to the protected portions of the data other than in a non-useable form; and permitting a user access to the data only in accordance with the rules as enforced by a tamper detecting mechanism.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 8-16	In another preferred embodiment, this invention is a	No teaching or

	device for controlling access to digital data, the digital data comprising protected data portions and rules concerning access rights to the digital data. The device includes storage means for storing the rules; and means for accessing the protected data portions only in accordance with the rules, whereby user access to the protected data portions is permitted only if the rules indicate that the user is allowed to access the portions of the data.	suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 17-27	In another aspect, this invention is a method of distributing digital data for subsequent controlled use of the data by a user. The method includes protecting portions of the digital data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing the protected portions of the digital data and the protected rules. The user is provided controlled access to the data only in accordance with the rules as enforced by a tamper detecting access mechanism.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 28-34	In another aspect, this invention is a storage device, readable by a machine, tangibly embodying a package of digital data comprising protected portions of digital data; and rules concerning access rights to the digital data, whereby a user is provided controlled access to the digital data only in accordance with the rules as enforced by a tamper detecting access mechanism.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 35-39	The data represent computer software, text, graphics, audio, and video, alone or in combinations. The protecting is done by encrypting the portions of the data, and access is prevented to the encrypted portions of the data other than in encrypted form.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 40-43	In some embodiments the rules are provided with the data, whereas in others the rules are provided separately. The rules can specify various access rights and controls, including rights of further distribution of the data.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 44-45	In preferred embodiments, data are destroyed when tampering is detected.	No teaching or suggestion of a license manager configured to allocate an

		incentive as recited in claim 12
7, 46-50	The device containing the mechanism of the present invention can be a stand-alone device such as a facsimile machine, a television, a VCR, a laser printer, a telephone, a laser disk player, a computer system or the like.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 51-55	As noted above, the rules, policies and protections of data are typically made by the data owners and/or distributors based on their security analysis of various threats. The various threats listed above are dealt with by countermeasures in the present invention.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
7, 56 – 8, 13	Threat: Capture of Output Signal Countermeasure: Encrypt or Scramble Output Signal Protection of the output signal is accomplished with encryption of a digital signal (as is done in the present invention) and scrambling of an analog signal. This solution requires installing decryption or unscrambling capability in the output device, TV or monitor, along with appropriate tamper-detection capability. Encryption or scrambling might be effected using a public key associated with the output device (although, to prevent so-called "spoofing," obtained from a certification authority and not from the output device). Alternatively, the output might be encrypted or scrambled using a private key only available to the designated output device (again ensured via some certification mechanism). The output signal is decrypted or unscrambled by the output device using its private key and is not available in plaintext form outside of the device's protected enclosure. Countermeasure: Protect Output Signal by Packaging The output signal is protected by making it unavailable outside the access mechanism. A sealed-unit computer with tamper detection provides the necessary protection. Examples of the acceptability of such packaging include lap-top computers and the original Macintosh computer, as well as integrated televisions, VCRs and video or audio laser disk players.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12
8, 14-36	Threat: Digital Copying Countermeasure: Secure Coprocessor Selection of a secure coprocessor is indicated to	No teaching or suggestion of a license manager

	implement protection against unauthorized use when an operating system (OS) is determined to be untrustworthy--that is, when the OS cannot provide adequate resistance to the anticipated threat. When the OS is untrustworthy, any measures implemented in the OS, or protected by it, can be circumvented through the OS or by-passing it. Countermeasure: Detection of Unsealing The protection provided by a coprocessor could be circumvented by tampering. The coprocessor is protected by tamper detection that causes the rules, cryptographic data, and decrypted protected data to be destroyed. Both passive and active means are used to effect such destruction. Semiconductor memory is volatile and does not retain data when power is removed. A long-life battery provides energy sufficient to allow rewriting (zeroizing) nonvolatile memory containing, for example, the private key. Without the private key the system will be unable to decrypt any protected data and it must be returned to an authorized service facility for installation of a new private key.	configured to allocate an incentive as recited in claim 12
8, 37-57	Threat: Deliberate Attack via Legacy and Customized Hardware Countermeasure: Keep the Information on the Coprocessor Board Access may be controlled if the information leaves the coprocessor board only for output purposes. Deciphered information is retained in memory on the coprocessor board, not in main memory. Program execution occurs in the coprocessor on the board (e.g., operating in the same manner as did so-called "accelerator" coprocessors that allowed a user to install an 80286 processor in an 80186 system, allowing the user to shift all functions to or from the faster coprocessor using a software command). Where information must leave the coprocessor board, e.g., to be sent to an output device, it may, depending on the associated rules, be encrypted. To receive and process encrypted data, the output device must have an access mechanism as well as public and private keys and tamper detect capability. Because some output peripheral devices do not have the capability of retransmission, the device may be a subset of the full access mechanism associated with a processor or computer system.	No teaching or suggestion of a license manager configured to allocate an incentive as recited in claim 12

For at least these reasons, the Examiner's rejection of independent claim 12 under 35 U.S.C. § 102(b) over Schneck should be withdrawn.

2. Claims 13-20

Each of claims 13-20 incorporates the features of independent claim 12 and therefore is patentable for at least the same reasons explained above. Claims 17-20 also are patentable for the following additional reasons.

Claim 17 recites that a licensed distributor is configured to transmit to one or more portable media devices meta-data associated with broadcasted digital content and containing an embedded distributor identifier. Schneck does not expressly or impliedly teach such a feature. Indeed, none of the rules fields described in Schneck's approach contains an identifier of a distributor (see, e.g., FIG. 3 and Table 1 at col. 11, lines 6-35).

The Examiner has cited col. 7, lines 22-35, of Schneck's disclosure to support her rejection of claim 17. The totality of the cited disclosure is as follows:

> The method includes protecting portions of the digital data; preventing access to the protected portions of the data other than in a non-useable form; determining rules concerning access rights to the data; protecting the rules; and providing the protected portions of the digital data and the protected rules. The user is provided controlled access to the data only in accordance with the rules as enforced by a tamper detecting access mechanism.
>
> In another aspect, this invention is a storage device, readable by a machine, tangibly embodying a package of digital data comprising protected portions of digital data; and rules concerning access rights to the digital data, whereby a user is provided controlled access to the digital data only in accordance with the rules as enforced by a tamper detecting access mechanism.

Nowhere in this disclosure is there an explicit or inherent teaching or suggestion of a licensed distributor that is configured to transmit to one or more portable media devices meta-data associated with broadcasted digital content and containing an embedded distributor identifier.

Claims 18-20 incorporate the features of claim 17 and therefore are patentable for at least the same reasons.

For at least these additional reasons, the Examiner's rejection of dependent claims 17-20 under 35 U.S.C. § 102(b) over Schneck should be withdrawn.

III. Conclusion

For the reasons explained above, all of the pending claims are now in condition for allowance and should be allowed.

Charge any excess fees or apply any credits to Deposit Account No. 08-2025.

Respectfully submitted,

Date: January 8, 2004

Edouard Garcia
Reg. No. 38,461
Telephone No.: (650) 631-6591

Please direct all correspondence to:

Hewlett-Packard Company
Intellectual Property Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80528-9599